



(11)特許出願公開番号  
特開2002-204229  
(P2002-204229A)

(43)公開日 平成14年7月19日(2002.7.19)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
H 0 4 L 9/08		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0	H 0 4 L 9/00	6 0 1 C 5 J 1 0 4
			6 0 1 E

審査請求 未請求 請求項の数14 O L (全 15 頁)

(21)出願番号 特願2000-401376(P2000-401376)

(22)出願日 平成12年12月27日(2000. 12. 27)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 高木 聡

東京都品川区北品川6丁目7番35号ソニー  
株式会社内

(74)代理人 100082740

弁理士 田辺 恵基

Fターム(参考) 5B017 AA03 BA07

5J104 AA16 EA04 EA15 NA02

(54)【発明の名称】 暗号化装置、暗号化方法、暗号復号化装置、暗号復号化方法及び暗号化システム

(57) 【要約】

【課題】第三者によって暗号化対象を容易に解読されることを防止し得るようにする。

【解決手段】各素材が入力される度にその各素材をそれぞれ特定するためのUMIDデータD11を生成し、各素材にそれぞれ対応する当該UMIDデータD11を暗号化鍵D10の数学的条件に合わせる変換を行って各素材毎に固有な素材特定暗号化鍵D13を生成し、当該素材特定暗号化鍵D13で各素材毎に対応したそれぞれ異なるデータ並替パターン（シャフリングテーブルデータD14及びインターリーブテーブルデータD15）をそれぞれ暗号化して各素材に対応した暗号化データD16及びD17を生成することにより、第三者にとっては暗号化鍵D10のアルゴリズム、また素材毎に特定されたUMIDデータD11に基づいて素材特定暗号化鍵D13に変換する変換パターン、さらにはUMIDデータD11の全てが分からなければ到底解読し得ない素材特定暗号化鍵D13を生成し得る。

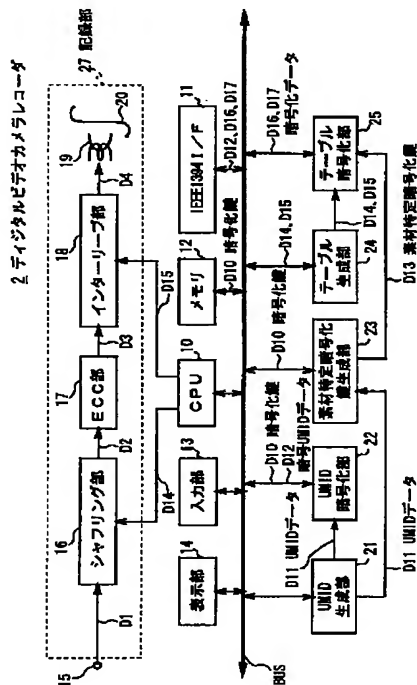


図2 デジタルビデオカメラコーダの構成

## 【特許請求の範囲】

【請求項 1】各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成する固有情報生成手段と、

上記各素材にそれぞれ対応する上記固有情報を所定的方式に従って変換することにより上記各素材毎に固有な暗号化鍵を生成する暗号化鍵生成手段と、

上記各素材にそれぞれ対応した上記暗号化鍵で上記各素材又は上記各素材に対応した所定の情報をそれぞれ暗号化する暗号化手段とを具えることを特徴とする暗号化装置。

【請求項 2】上記各素材に対応した所定の情報は、上記各素材が入力される度に当該各素材を所定データ量単位でそれぞれ並び替えるときのデータ並替パターンであることを特徴とする請求項 1 に記載の暗号化装置。

【請求項 3】上記固有情報生成手段は、少なくとも上記暗号化装置を管理するための管理情報に乱数を乗じることにより上記固有情報を生成することを特徴とする請求項 1 に記載の暗号化装置。

【請求項 4】各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成する固有情報生成ステップと、

上記各素材にそれぞれ対応する上記固有情報を所定的方式に従って変換することにより上記各素材毎に固有な暗号化鍵を生成する暗号化鍵生成ステップと、

上記各素材にそれぞれ対応した上記暗号化鍵で上記各素材又は上記各素材に対応した所定の情報をそれぞれ暗号化する暗号化ステップとを具えることを特徴とする暗号化方法。

【請求項 5】上記各素材に対応した所定の情報は、上記各素材が入力される度に当該各素材を所定データ量単位でそれぞれ並び替えるときのデータ並替パターンであることを特徴とする請求項 4 に記載の暗号化方法。

【請求項 6】上記固有情報生成ステップは、少なくとも上記暗号化装置を管理するための管理情報に乱数を乗じることにより上記固有情報を生成することを特徴とする請求項 4 に記載の暗号化方法。

【請求項 7】各素材が入力される度に当該各素材をそれぞれ特定するために生成された固有情報と、当該固有情報に基づく上記各素材毎に固有な暗号化鍵で上記各素材又は上記各素材に対応した所定の情報をそれぞれ暗号化することにより生成された暗号化データとを上記暗号化装置から取得する取得手段と、

上記各素材にそれぞれ対応する上記固有情報を所定的方式に従って変換することにより上記暗号化データをそれぞれ復号化するための復号化鍵を生成する復号化鍵生成手段と、

上記各素材にそれぞれ対応する上記復号化鍵で上記暗号化データをそれぞれ復号化することにより上記各素材又は上記各素材に対応した所定の情報を復元する暗号復号

化手段とを具えることを特徴とする暗号復号化装置。

【請求項 8】各素材が入力される度に当該各素材をそれぞれ特定するために生成された固有情報と、当該固有情報に基づく上記各素材毎に固有な暗号化鍵で上記各素材又は上記各素材に対応した所定の情報をそれぞれ暗号化することにより生成された暗号化データとを上記暗号化装置から取得する取得ステップと、

上記各素材にそれぞれ対応する上記固有情報を所定的方式に従って変換することにより上記暗号化データをそれぞれ復号化するための復号化鍵を生成する復号化鍵生成ステップと、

上記各素材にそれぞれ対応する上記復号化鍵で上記暗号化データをそれぞれ復号化することにより上記各素材又は上記各素材に対応した所定の情報を復元する暗号復号化ステップとを具えることを特徴とする暗号復号化方法。

【請求項 9】暗号化装置と暗号復号化装置とで構築される暗号化システムにおいて、上記暗号化装置は、

各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成する固有情報生成手段と、

上記各素材にそれぞれ対応する上記固有情報を所定的方式に従って変換することにより上記各素材毎に固有な暗号化鍵を生成する暗号化鍵生成手段と、

上記各素材にそれぞれ対応した上記暗号化鍵で上記各素材又は上記各素材に対応した所定の情報をそれぞれ暗号化することにより暗号化データを生成する暗号化手段と、

上記各素材にそれぞれ対応する上記固有情報と上記暗号化データとを送信する送信手段とを具え、

上記暗号復号化装置は、上記各素材にそれぞれ対応する上記固有情報と上記暗号化データとを受信する受信手段と、

上記各素材にそれぞれ対応する上記固有情報を所定的方式に従って変換することにより上記暗号化データをそれぞれ復号化するための復号化鍵を生成する復号化鍵生成手段と、

上記各素材にそれぞれ対応する上記復号化鍵で上記暗号化データをそれぞれ復号化することにより上記各素材又は上記各素材に対応した所定の情報を復元する暗号復号化手段とを具えることを特徴とする暗号化システム。

【請求項 10】上記各素材に対応した所定の情報は、上記各素材が入力される度に当該各素材を所定データ量単位でそれぞれ並び替えるときのデータ並替パターンであることを特徴とする請求項 9 に記載の暗号化システム。

【請求項 11】上記固有情報生成手段は、少なくとも上記暗号化装置を管理するための管理情報に乱数を乗じることにより上記固有情報を生成することを特徴とする請求項 9 に記載の暗号化システム。

【請求項 12】暗号化装置と暗号復号化装置とで構築さ

れる暗号化システムにおいて、  
 上記暗号化装置は、  
 各素材が入力される度に当該各素材をそれぞれ特定する  
 ための固有情報を生成する固有情報生成手段と、  
 上記各素材にそれぞれ対応する上記固有情報を所定の方  
 式に従って変換することにより上記各素材毎に固有な暗  
 号化鍵を生成する暗号化鍵生成手段と、  
 上記各素材にそれぞれ対応した上記暗号化鍵で上記各素  
 材又は上記各素材に対応した所定の情報をそれぞれ暗号  
 化することにより暗号化データを生成する暗号化手段 10  
 と、  
 上記各素材にそれぞれ対応する上記固有情報と上記暗号  
 化データとを所定の記憶媒体に記録する記憶手段とを具  
 え、  
 上記暗号復号化装置は、  
 上記記憶媒体から上記各素材にそれぞれ対応する上記固  
 有情報と上記暗号化データとを読み出す読み出し手段  
 と、  
 上記各素材にそれぞれ対応する上記固有情報を所定の方  
 式に従って変換することにより上記暗号化データをそれ  
 ぞれ復号化するための復号化鍵を生成する復号化鍵生成  
 手段と、  
 上記各素材にそれぞれ対応する上記復号化鍵で上記暗号  
 化データをそれぞれ復号化することにより上記各素材又  
 は上記各素材に対応した所定の情報を復元する暗号復号  
 化手段とを具えることを特徴とする暗号化システム。

【請求項 13】 上記各素材に対応した所定の情報は、上  
 記各素材が入力される度に当該各素材を所定データ量  
 単位でそれぞれ並び替えるときのデータ並替パターンで  
 あることを特徴とする請求項 12 に記載の暗号化システ  
 ム。 20

【請求項 14】 上記固有情報生成手段は、  
 少なくとも上記暗号化装置を管理するための管理情報に  
 乱数を乗じることにより上記固有情報を生成することを  
 特徴とする請求項 12 に記載の暗号化システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は暗号化装置、暗号化  
 方法、暗号復号化装置、暗号復号化方法及び暗号化シス  
 テムに関し、例えばデジタルビデオカメラレコーダと  
 デジタルビデオテープレコーダとで構築される暗号化  
 システムに適用して好適なものである。 40

【0002】

【従来の技術】 従来、デジタルビデオテープレコーダ  
 （以下、これをビデオテープレコーダと呼ぶ）は、撮影  
 者の操作によりデジタルビデオカメラレコーダ（以  
 下、これをビデオカメラと呼ぶ）でビデオカセットの磁  
 気テープに記録された画像データを再生することにより  
 外部モニタに再生映像を表示するようになされている。

【0003】 しかしながらビデオテープレコーダにおい 50

ては、撮影者の意図しない第三者によって再生操作され  
 た場合でも、再生映像を外部モニタに表示してしまうの  
 で、意図しない第三者に容易に当該再生映像が視認され  
 てしまっていた。

【0004】 このような問題を解決する 1 つの方法とし  
 ては、撮像することにより得られた画像データに対して  
 所定の暗号アルゴリズムに基づく暗号化処理を施した後  
 にビデオカセットの磁気テープに記録するビデオカメラ  
 と、そのビデオカセットを再生する際、当該ビデオカメ  
 ラの場合と同じ暗号アルゴリズムに基づく復号化処理を  
 施すことにより元の画像データを復元するビデオテー  
 プレコーダとで暗号化システムを構築することが考えられ  
 る。

【0005】

【発明が解決しようとする課題】 ところがかかる暗号化  
 システムにおいては、ビデオカメラによって常時同じ暗  
 号アルゴリズムに基づく暗号化処理を施しているの  
 で、その暗号アルゴリズムが意図しない第三者によって解読  
 された場合には、そのビデオカメラで撮像されたビデオ  
 カセットの再生映像が全てビデオテープレコーダを介し  
 て視認されてしまうという問題がある。

【0006】 本発明は以上の点を考慮してなされたもの  
 で、第三者によって容易に暗号化対象が解読されること  
 を防止し得る暗号化装置、暗号化方法、暗号復号化装  
 置、暗号復号化方法及び暗号化システムを提案しようと  
 するものである。

【0007】

【課題を解決するための手段】 かかる課題を解決するた  
 め本発明においては、各素材が入力される度に当該各素  
 材をそれぞれ特定するための固有情報を生成し、各素材  
 にそれぞれ対応する固有情報を所定の方式に従って変換  
 して各素材毎に固有な暗号化鍵を生成し、その暗号化鍵  
 で各素材又は各素材に対応した所定の情報をそれぞれ暗  
 号化することにより、類推し難い固有情報の全てが分か  
 らなければ第三者にとっては到底解読し得ない固有な素  
 材毎の暗号化鍵を生成することができるので、当該第三  
 者によって容易に暗号化対象が解読されることを防止し  
 得る。

【0008】 また各素材毎に対応した所定の情報とし  
 て、各素材が入力される度にその各素材を所定データ量  
 単位でそれぞれ並び替えるためのデータ並替パターンを  
 暗号化するようにしたことにより、素材そのものを暗号  
 化するよりも一段と少ないデータ量で暗号化することが  
 できる。

【0009】 またかかる課題を解決するため本発明にお  
 いては、各素材が入力される度に当該各素材をそれぞれ  
 特定するために生成された固有情報と、当該固有情報に  
 基づく各素材毎に固有な暗号化鍵で各素材又は各素材に  
 対応した所定の情報をそれぞれ暗号化して生成された暗  
 号化データとを暗号化装置から取得し、各素材にそれぞ

れ対応する固有情報を所定の方式に従って変換して暗号化データをそれぞれ復号化するための復号化鍵を生成し、その復号化鍵で暗号化データをそれぞれ復号化して各素材又は各素材に対応した所定の情報を復元することにより、類推し難い固有情報と、当該固有情報に基づいて生成されているために第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵とを取得して復号化鍵を生成することができるので、確実かつ正確に各素材又は各素材に対応した所定の情報毎を復元し得る。

【0010】さらにかかる課題を解決するため本発明においては、各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して各素材毎に固有な暗号化鍵を生成し、その暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化して暗号化データを生成し、暗号化データと固有情報とを送信する暗号化装置と、当該暗号化データと固有情報とを受信し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して暗号化データをそれぞれ復号化するための復号化鍵を生成し、その復号化鍵で暗号化データをそれぞれ復号化して各素材又は各素材に対応した所定の情報を復元する暗号復号化装置とを構築することにより、暗号化装置では、類推し難い固有情報の全てが分からなければ第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵を生成することができるので、当該第三者によって容易に暗号化対象が解読されることを防止し得、暗号復号化装置では、送信手段を介して類推し難い固有情報と、当該固有情報に基づいて生成されているために第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵とを受信して復号化鍵を生成することができるので、確実かつ正確に各素材又は各素材に対応した所定の情報毎を復元し得る。

【0011】さらにかかる課題を解決するため本発明においては、各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して各素材毎に固有な暗号化鍵を生成し、その暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化して暗号化データを生成し、暗号化データと固有情報とを所定の記憶媒体に記憶する暗号化装置と、その暗号化データと固有情報とを当該記憶媒体から読み出し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して暗号化データをそれぞれ復号化するための復号化鍵を生成し、その復号化鍵で暗号化データをそれぞれ復号化して各素材又は各素材に対応した所定の情報を復元する暗号復号化装置とを構築することにより、暗号化装置では、類推し難い固有情報の全てが分からなければ第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵を生成することができるので、当該第三者によって容易に暗号化対象が解読されることを防止し得、暗号復号化装

置では、記憶手段から読み出した類推し難い固有情報と、当該固有情報に基づいて生成されているために第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵とを受信して復号化鍵を生成することができるので、確実かつ正確に各素材又は各素材に対応した所定の情報毎を復元し得る。

【0012】

【発明の実施の形態】以下図面について、本発明の一実施の形態を詳述する。

【0013】(1) ネットワーク対応型暗号化システム図1において、1は全体として本発明によるネットワーク対応型暗号化システムを示し、デジタルビデオカメラレコーダ(以下、これをビデオカメラと呼ぶ)2と、デジタルビデオテープレコーダ(以下、これをビデオテープレコーダと呼ぶ)3とが互いにパーソナルコンピュータ(図示せず)を介してそれぞれインターネット4に接続されており、デジタルビデオカメラ2とビデオテープレコーダ3との間で各種情報の授受を行い得るようになされている。

【0014】このネットワーク対応型暗号化システム1では、ビデオカメラ2において撮像して得られた素材である画像データに所定の処理を施して記録したビデオカセット5がビデオテープレコーダ3に装填されて再生されるようになされている。

【0015】(2) ビデオカメラにおける暗号化処理手順

図2に示すような回路構成のビデオカメラ2を用いて本実施の形態における暗号化処理手順を説明する。

【0016】このビデオカメラ2は、CPU(Central Processing Unit)10、他の機器(本実施の形態の場合はパーソナルコンピュータ)との間で各種情報の授受を行うIEEE(Institute of Electrical and Electronics Engineers)1394インターフェイス(I/F)11、メモリ12、各種操作ボタン(図示せず)等の設けられた入力部13、液晶ディスプレイでなる表示部14及び暗号化部26がそれぞれデータバスBUSを介して互いに接続されており、当該CPU10がメモリ12から読み出した各種プログラムに従って所定の処理を実行することによりビデオカメラ2を統括的に制御し、記録部27によりビデオカセット5(図1)の磁気テープ20に対して記録処理を実行するようになされている。

【0017】實際上、図3において、CPU10は、ルーチンRT1に従った暗号化処理手順の開始ステップからステップSP1に移る。

【0018】ステップSP1においてCPU10は、まず最初にビデオテープレコーダ3からインターネット4(図1)を経由して送信された非対象暗号化方式であるRSAに従った暗号化鍵D10をIEEE1394インターフェイス11を介して予め取得してメモリ12に記憶し、次のステップSP2に移る。

【0019】ステップSP2においてCPU10は、入力部13の記録ボタンが撮影者によって押下されたか否かを判断する。ここで否定結果が得られると、CPU10は記録ボタンが押下されるまで待ち受ける。これに対して肯定結果が得られると、CPU10は次のステップSP3に移る。

【0020】ステップSP3においてCPU10は、UMID生成部21によって、メモリ12に記憶されている各種情報やシステムクロック等に基づいて画像データや音声データ等の素材を特定するためのUMID(Unique Material Identifier)を生成し、当該UMIDのうち一部分をUMIDデータD11として抽出し、これをUMID暗号化部22及び素材特定暗号化鍵生成部23に送出し、次のステップSP4に移る。

【0021】ここで、UMIDのデータ構造について説明する。図4において、UMIDは、基本UMIDと延長UMIDとの64 [byte]から構成され、基本UMIDは当該UMIDであること等を表す12 [byte]のユニバーサルラベル、データの長さを表す1 [byte]のデータ長、ダビング回数を表す3 [byte]のインストナンプ及びビデオカメラ2もしくはそのビデオカメラ2内のチップ固有のシリアルナンバに乱数を乗じることにより固有な情報として生成された16 [byte]のマテリアルナンバを含む全32 [byte]で構成される。

【0022】また延長UMIDは、ビデオカメラ2内のシステムクロックに基づく日及び時刻を表す8 [byte]の日時、GPS(Global Positioning System)機能を有するビデオカメラの場合には、そのビデオカメラの存在位置を表す12 [byte]の位置情報、国を表す4 [byte]の国コード、組織を表す4 [byte]の組織コード及びユーザを表す4 [byte]のユーザ名を含む全32 [byte]で構成される。

【0023】この実施の形態の場合、CPU10は、かかるUMIDのうち固有な情報であるマテリアルナンバを含む基本UMIDをUMIDデータD11として抽出するようになされており、当該マテリアルナンバによって素材を特定し得るようになされている。

【0024】このようにCPU10は、撮影者によって記録ボタンが押下される毎に素材を特定するための新たなUMIDデータD11を生成するようになされている。

【0025】ステップSP4においてCPU10は、メモリ12に記憶しておいた暗号化鍵D10をUMID暗号化部22及び素材特定暗号化鍵生成部23に送出し、次のステップSP5に移る。

【0026】ステップSP5においてCPU10は、素材特定暗号化鍵生成部23によって、素材を特定するためのUMIDデータD11を暗号化鍵D10に基づく数学的条件に合わせて変換することにより、素材固有の暗号化鍵である素材特定暗号化鍵D13を生成する。

【0027】またCPU10は、UMID暗号化部22によって、ビデオテープレコーダ3において素材特定暗号化鍵D13を復号化するために必要なUMIDデータD11に対して、ビデオテープレコーダ3から送信された暗号化鍵D10で暗号化処理を施して暗号UMIDデータD12を生成することにより、インターネット4を経由してビデオテープレコーダ3に送信する際、第三者によって解読されることを防止し得るようになされている。

【0028】そしてCPU10は、素材特定暗号化鍵D13をテーブル暗号化部25に送出すると共に、暗号UMIDデータD12を一旦メモリ12に記憶した後、次のステップSP6に移る。

【0029】ステップSP6においてCPU10は、例えば図5に示すようなパターン決定画面14Aを表示部14に表示し、シャフリング部16及びインターリーブ部18においてデータ列の並び替えを行う際のデータ並替パターンの決定を撮影者に対して促す。

【0030】そしてCPU10は、パターン決定画面14Aを介して第1のパターン(シャフリング)項目14B及び第2のパターン(インターリーブ)項目14Cからそれぞれ所望のパターン番号が撮影者によって入力部13から選択操作されると、当該選択された各パターン番号に対応したデータ並替パターンであるシャフリングテーブルデータD14及びインターリーブテーブルデータD15をテーブル生成部24により例えば16 Modulo 4の関数に従って任意に生成し、次のステップSP7に移る。

【0031】因みに、CPU10は、記録ボタンが押下される毎に新たに生成するUMIDデータD11と同様、記録ボタンが押下される毎にデータ並替パターンを撮影者に選択させることにより、素材毎に新たなシャフリングテーブルデータD14及びインターリーブテーブルデータD15を生成するようになされている。

【0032】ステップSP7においてCPU10は、シャフリングテーブルデータD14をシャフリング部16に送出し、インターリーブテーブルデータD15をインターリーブ部18に送出することにより、シャフリング部16及びインターリーブ部18に対してそれぞれデータ並替パターンを設定すると共に、当該シャフリングテーブルデータD14及びインターリーブテーブルデータD15をテーブル生成部24からテーブル暗号化部25に送出し、次のステップSP8に移る。

【0033】ステップSP8においてCPU10は、テーブル暗号化部25によって、シャフリング部16及びインターリーブ部18でそれぞれ設定したシャフリングテーブルデータD14及びインターリーブテーブルデータD15に対して、素材特定暗号化鍵生成部23から供給された素材固有の暗号化鍵である素材特定暗号化鍵D13で暗号化処理を施すことにより、インターネット4

(図1)を経由してビデオテープレコーダ3へ送信する際に第三者に解読されることがないように暗号化データD16及びD17を生成し、これらを一旦メモリ12に記憶した後、次のステップSP9に移る。

【0034】ステップSP9においてCPU10は、上述のステップSP2で記録ボタンが押下されたことにより撮像して得られた素材である画像データに対してMP EG 2 (Moving Picture Experts Group-layer 2)方式の圧縮符号化処理が施されたエレメンタルストリームD1を入力端15を介して記録部27のシャフリング部16

10 に入力する。  
【0035】シャフリング部16は、上述のステップSP7で設定されたシャフリングテーブルデータD14のデータ並替パターンに従って、エレメンタルストリームD1の1フレーム分の各マクロブロックを並び替えるシャフリングを施す。

【0036】このシャフリングの主たる目的としては、磁気テープ上へのマクロブロックの記録位置を分散させることにより、記録時とは異なるテープ速度で再生する変速再生時において、訂正し得なかったエラーが生じたときに再生映像を極力見易くすることにある。

【0037】因みに、マクロブロックとは、MPEG 2のデータ構造のうち、16ライン×16画素のY(輝度)信号ブロック4個と、当該Y信号ブロック4個に対応する16ライン×16画素のCr( R(赤)成分とY成分との色差成分)信号及びCb( B(青)成分とY成分との色差成分)信号各1ブロックから構成される単位をいう。このマクロブロックは、可変長符号化されていることにより、各々のデータの長さが不揃いである。

【0038】實際上シャフリング部16で行われるシャフリング処理を図6及び図7において概略的に説明する。但し説明上の簡素化のため、以下、1フレームに9マクロブロックだけが含まれているものと仮定する。

【0039】図6において、シャフリング部16は、走査順に並ぶ各マクロブロックMB1~MB9を、テーブル生成部24から供給されたシャフリングテーブルデータD14に従って、予め指定された内部メモリのメモリマップヘランダムに書き込むことによりシャフリングを施す。

【0040】このときシャフリング部16は、図7に示すように、可変長データである各マクロブロックを、磁気テープ20上に記録する際の単位である固定長枠(以下、これをシンクブロックと呼ぶ)に分割し、当該シンクブロックよりも長い各オーバーフロー部MB5'、MB2'及びMB3'を一旦バッファリングし、シンクブロックに満たない(空きのある領域)マクロブロックMB8、MB1、MB7及びMB6の後ろに各オーバーフロー部MB5'、MB2'及びMB3'を順に詰め込むことにより固定長である各シンクブロックSK1~SK9を生成する。

【0041】そしてシャフリング部16は、各シンクブロックSK1~SK9を上位又は下位番地から順に読み出し、これをVLC(Variable Length Code)データD2としてECC(Error Correctig Code)部17(図2)に送出する。

【0042】ECC部17は、図8に示すように、シャフリング部16から供給されたVLCデータD2のシンクブロックSK1~SK9を2次的に配列し、まず垂直方向に演算してリードソロモン符号(以下、これを外符号データと呼ぶ)PB1~PB3を生成し、次に水平方向に演算してリードソロモン符号(以下、これを内符号データと呼ぶ)PB4~PB7を生成する。

【0043】そしてECC部17は、外符号データPB1~PB3及び内符号データPB4~PB7をVLCデータD2に付加することにより誤り訂正符号付加データD3を生成し、これをインターリーブ部18(図2)に送出する。

【0044】インターリーブ部18は、上述のステップSP7で設定されたインターリーブテーブルデータD15のデータ並替パターンに従って、ECC部17から供給された誤り訂正符号付加データD3の各シンクブロックSK1~SK9、外符号データPB1~PB3及び内符号データPB4~PB7を予め指定された内部メモリのメモリマップヘランダムに書き込むことによりインターリーブを施す。

【0045】このインターリーブの主たる目的としては、バースト誤りの影響を分散させ、誤り訂正能力を極力ランダム誤りの訂正能力に近づけることや、訂正不可能となった誤りに対して精度良好な誤り修整(コンシールメント)を行い得るようにすることである。

【0046】因みに、バースト誤りはビット毎に独立することなく、集中的に発生する誤りのことであり、ランダム誤りは各ビット毎に不規則に生ずる誤りのことである。さらに誤り修整(コンシールメント)は、訂正不可能となった誤りによる画面上での視覚的劣化部分近傍の誤りのない画素を用いて、補間処理を施すことである。

【0047】インターリーブ部18は、インターリーブを施した状態において、ランダムに書き込んだ各シンクブロックSK1~SK9、外符号データPB1~PB3及び内符号データPB4~PB7を上位又は下位番地から順に読み出し、これを記録画像データD4として磁気ヘッド19を介して磁気テープ20に記録する。

【0048】このようにしてCPU10は、ステップSP9における記録処理を実行し、次のステップSP10に移る。

【0049】ステップSP10においてCPU10は、入力部13の停止ボタンが押下されたか否かを判断する。ここで否定結果が得られると、CPU10はステップSP9に戻って記録処理を続ける。

【0050】これに対して肯定結果が得られると、CP



U10は記録処理を停止し、次のステップSP11に移る。

【0051】この場合、磁気テープ20に記録された記録画像データD4をビデオテープレコーダ3が再生するには、記録画像データD4を生成する過程で行ったデータ並替パターン（シャフリングテーブルデータD14及びインターリーブテーブルデータD15）を認識し、当該データ並替パターンとは逆のデータ並戻パターンを用いてデータの並び戻しを行う必要がある。

【0052】従ってCPU10は、上述のステップSP5でメモリ12に一旦記憶した暗号UMIDデータD12と、上述のステップSP8でメモリ12に一旦記憶した暗号化データD16及びD17とをビデオテープレコーダ3に送信しなければならない。

【0053】ステップSP11においてCPU10は、メモリ12に一旦記憶していた暗号UMIDデータD12、暗号化データD16及びD17をメモリ12から読み出し、これらをIEEE1394インターフェイス11からパーソナルコンピュータ（図示せず）及びインターネット4（図1）を順次介してビデオテープレコーダ3に送信した後、再度ステップSP2に移って、上述の処理を繰り返す。

【0054】このように、ビデオカメラ2は、上述のルーチンRT1の暗号化処理手順を入力部13の記録ボタンが押下される度に繰り返すことにより、図9に示すように、当該記録ボタンが押下される度に入力された素材毎にそれぞれ異なるデータ並替パターンでデータ列の並び替えを行って生成した記録画像データD4（D4A～D4N）を順次磁気テープ20に記録するようになされている。

【0055】さらにCPU10は、記録ボタンが押下される度に入力された素材毎にそれぞれを特定するためのUMIDデータD11を暗号化鍵D10で暗号化することにより暗号UMIDデータD12（D12A～D12N）を生成すると共に、そのUMIDデータD11を暗号化鍵D10の数学的条件に合わせる変換を行うことにより素材毎に固有な素材特定暗号化鍵D13を生成し、当該素材特定暗号化鍵D13でそれぞれ対応するデータ並替パターンを暗号化することにより暗号化データD16（D16A～D16N）、D17（D17A～D17N）を生成し得るようになされている。

【0056】このようにしてCPU10は、磁気テープ20に記録した記録画像データD4（D4A～D4N）をビデオテープレコーダ3で再生するために必要な暗号UMIDデータD12（D12A～D12N）及び暗号化データD16（D16A～D16N）、D17（D17A～D17N）を当該記録画像データD4（D4A～D4N）に対応させて生成し、これらを一旦メモリ12に記憶しておき、記録処理が全て終了した後にパーソナルコンピュータ及びインターネット4（図1）を介して

ビデオテープレコーダ3に送信するようになされている。

【0057】かくしてCPU10は、記録画像データD4（D4A～D4N）に対応したデータ並替パターン（シャフリングテーブルデータD14及びインターリーブテーブルデータD15）を暗号化していることにより、その暗号化前のデータ並替パターンをビデオテープレコーダ3が認識できない限り元の素材に戻すことができず再生できないので、結果として素材毎に暗号化することができる。

【0058】（3）ビデオテープレコーダにおける復号化処理手順

図10に示すような回路構成のビデオテープレコーダ3を用いて本実施の形態における復号化処理手順を説明する。

【0059】このビデオテープレコーダ3は、CPU30、他の機器（本実施の形態の場合はパーソナルコンピュータ）との間で各種情報の授受を行うIEEE1394インターフェイス31、メモリ32、HDD（ハードディスクドライブ）33、各種操作ボタン（図示せず）等の設けられた入力部34、及びビデオカメラ2に送信するための暗号化鍵D10やその暗号化鍵D10に対応する復号化鍵D20を生成する鍵生成部40がそれぞれデータバスBUSを介して互いに接続されており、当該CPU30がHDD33から読み出した各種プログラムに従って所定の処理を実行することによりビデオテープレコーダ3を統括的に制御し、装填されたビデオカセット5を再生部45を介して再生するようになされている。

【0060】因みに鍵生成部40は、ビデオカメラ2に送信した暗号化鍵D10に対応する復号化鍵D20を生成し、これを予めHDD33に記録しておくようになされている。

【0061】實際上、CPU30は、ルーチンRT2に従った復号化処理手順の開始ステップから次のステップSP12に移る。

【0062】ステップSP12においてCPU30は、ビデオカメラ2からインターネット4を経由して送信された暗号UMIDデータD12A～D12N、暗号化データD16A～D16N及びD17A～D17NをIEEE1394インターフェイス31を介して取得してHDD33に記憶し、次のステップSP13に移る。

【0063】ステップSP13においてCPU30は、入力部34の再生ボタンが押下されたか否かを判断する。ここで否定結果が得られると、CPU30は再生ボタンが押下されるまで待ち受ける。これに対して肯定結果が得られると、CPU30は次のステップSP14に移る。

【0064】ステップSP14においてCPU30は、HDD33に予め記憶しておいた復号化鍵D20をUM



I D復号化部41及び素材特定復号化鍵生成部42に送出する。

【0065】そしてCPU30は、HDD33に記憶した暗号UMIDデータD12A～D12Nのうち最初に再生する素材である記録画像データD4Aに対応する暗号UMIDデータD12AをUMID復号化部41に送出すると共に、暗号化データD16A及びD17Aを素材特定復号化鍵生成部42に送出し、次のステップSP15に移る。

【0066】ステップSP15においてCPU30は、UMID復号化部41により暗号UMIDデータD12Aに対してHDD33から供給された復号化鍵D20で復号化処理を施すことにより、元のUMIDデータD11を復元し、これを素材特定復号化鍵生成部42に送出し、次のステップSP16に移る。

【0067】ステップSP16においてCPU30は、素材特定復号化鍵生成部42によりUMIDデータD11を復号化鍵D20に基づく数学的条件に合わせて変換することにより、ビデオカメラ2において生成された素材特定暗号化鍵D13に対応する素材特定復号化鍵D21を生成し、これをテーブル復号化部43に送出し、次のステップSP17に移る。

【0068】ステップSP17においてCPU30は、テーブル復号化部43により暗号化データD16A及びD17Aを素材特定復号化鍵生成部42から供給された素材特定復号化鍵D21でそれぞれ復号化処理を施すことにより、元のデータ並替パターンであるシャフリングテーブルデータD14及びインターリーブテーブルデータD15を復元し、次のステップSP18に移る。

【0069】ステップSP18においてCPU30は、シャフリングテーブルデータD14及びインターリーブテーブルデータD15にそれぞれ対応したデータ並戻パターンであるデシャフリングテーブルデータD22及びデインターリーブテーブルデータD23をHDD33から読み出す。

【0070】そしてCPU30は、デシャフリングテーブルデータD22をデシャフリング部36に送出すると共に、デインターリーブテーブルデータD23をデインターリーブ部38に送出することにより、デシャフリング部36及びデインターリーブ部38に対してそれぞれデータ並戻パターンを設定し、ステップSP19に移る。

【0071】ステップSP19においてCPU30は、再生ボタンの押下によりビデオカセット5(図1)の磁気テープ20から磁気ヘッド39を介して再生された最初の記録画像データD4Aをデインターリーブ部38に入力する。

【0072】デインターリーブ部38は、記録画像データD4Aを上記のステップSP18で設定されたデインターリーブテーブルデータD23に従って、インターリ

ーブとは逆パターンとなるデインターリーブを施すことにより元の誤り訂正符号付加データD3を復元し、これをECC部37に送出する。

【0073】ECC部37は、デインターリーブ部38から供給された誤り訂正符号付加データD3の内符号データPB4～PB7(図8)による誤り訂正処理を施した後、外符号データPB1～PB3(図8)による誤り訂正処理をも施すことにより、元のVLCデータD2を復元し、これをデシャフリング部36に送出する。

【0074】デシャフリング部36は、ECC部37から供給されたVLCデータD2を上記のステップSP18で設定されたデシャフリングテーブルデータD22に従って、シャフリングとは逆パターンとなるデシャフリングを施すことにより元のエレメンタルストリームD1を復元し、これを外部モニタに出力する。

【0075】因みに再生部45は、データ並替パターンを認識し得ない場合には、記録画像データD4を元のエレメンタルストリームD1に復元できず、その結果、外部モニタは画質の劣化どころか、再生者が認識し得ない映像を表示してしまうことになる。

【0076】このようにしてCPU30は、ステップSP19において最初の素材に対応する記録画像データD4Aに対する再生処理を実行し、次のステップSP20に移る。

【0077】ステップSP20においてCPU30は、ビデオカセット5の磁気テープ20から再生する記録画像データD4Aが次の新たな素材に対応する記録画像データD4Bになったか否かを判断する。

【0078】ここで肯定結果が得られると、このことは1本のビデオカセット5(図1)の磁気テープ20に記録された複数の記録画像データD4のうち最初の記録画像データD4Aの再生が終了したことを表しており、このときCPU30は再度ステップSP14に戻って、次の新たな記録画像データD4Bに対応する暗号UMIDデータD12B、暗号化データD16B及びD17BをUMID復号化部41及び素材特定復号化鍵生成部42に送出し、上記の処理を繰り返し、新たな素材に対応する記録画像データD4Bに対する再生処理を実行する。

【0079】このようにしてCPU30は、各素材に対応する記録画像データD4(D4A～D4N)が順次再生し終わる度に、次の素材に対応する暗号UMIDデータD12(D12A～D12N)及び暗号化データD16(D16A～D16N)、暗号化データD17(D17A～D17N)をUMID復号化部41及び素材特定復号化鍵生成部42に送出し、上記の処理を繰り返し、記録画像データD4(D4A～D4N)に対する再生処理を実行するようになされている。

【0080】これに対して否定結果が得られると、このことは磁気テープ20に記録された最初の素材に対応する記録画像データD4Aの再生が終了していないことを

表しており、このときCPU30は次のステップSP21に移る。

【0081】ステップSP21においてCPU30は、ビデオカセット5(図1)の磁気テープ20を最後まで再生したか否かを判断する。ここで否定結果が得られると、このことは記録画像データD4A~D4N全ての再生が未だ終了しておらず、再生途中であることを表しており、このときCPU30は、再度ステップSP19に戻って再生処理を続ける。

【0082】これに対して肯定結果が得られると、このことはビデオカセット5の磁気テープ20に記録された素材である記録画像データD4A~D4N全ての再生を終了したことを表しており、このときCPU30は再生処理を停止し、ステップSP22に移って復号化処理手順を終了する。

【0083】このようにCPU30は、各素材に対応する記録映像データD4A~D4Nを再生するために必要である暗号UMIDデータD12A~D12N及び暗号化データD16A~D16N、D17A~D17NをIEEE1394インターフェイス31を介して取得し、記録映像データD4A~D4Nを順次再生する度に、その記録画像データD4に対応する暗号UMIDデータD12を復号化鍵D20で復号化して得られたUMIDデータD11に基づく素材特定暗号化鍵D13で当該素材に対応する暗号化データD16及びD17を順次復号化することにより元のデータ並替パターンであるシャフリングテーブルデータD14及びインターリーブテーブルデータD15を復元することができる。

【0084】その結果CPU30は、シャフリングテーブルデータD14及びインターリーブテーブルデータD15に対応するデータ並替パターンであるデシャフリングテーブルデータD22及びインターリーブテーブルデータD23を用いて1本のビデオカセット5の磁気テープ20に記録された記録映像データD4A~D4Nをそれぞれ素材毎に順次再生することができる。

【0085】以上の構成において、ネットワーク対応型暗号化システム1におけるビデオカメラ2は、各素材が入力される度にその各素材をそれぞれ特定するためのUMIDデータD11を生成し、各素材にそれぞれ対応する当該UMIDデータD11を暗号化鍵D10の数学的条件に合わせる変換を行うことにより各素材毎に固有な素材特定暗号化鍵D13を生成する。

【0086】この素材特定暗号化鍵D13は、素材毎に類推され難い固有な情報(UMIDデータD11に含まれるマテリアルナンバ)を暗号化鍵D10の数学的条件に合わせる変換が行われているので、第三者にとっては暗号化鍵D10のアルゴリズム、また素材毎に特定されたUMIDデータD11に基づいて素材特定暗号化鍵D13に変換する変換パターン、さらにはUMIDデータD11に含まれる固有な情報(マテリアルナンバ)の全

てが分からなければ到底解読し得ない情報である。

【0087】そしてビデオカメラ2は、かかる素材特定暗号化鍵D13で各素材毎に対応したそれぞれ異なるデータ並替パターン(シャフリングテーブルデータD14及びインターリーブテーブルデータD15)をそれぞれ暗号化することにより、各素材に対応した暗号化データD16及びD17を生成する。

【0088】ここで、データ並替パターンは、磁気テープ20に記録され記録される前の過程で素材を並び替えるものであり、ビデオテープレコーダ3が再生するにはそのデータ並替パターンが分からなければ元の素材に復元できないので、記録画像データD4を再生するために必要不可欠な情報である。

【0089】従ってビデオカメラ2は、記録画像データD4そのものよりも一段と少ないデータ量であるデータ並替パターンを暗号化するだけで、あたかも記録画像データD4そのものを暗号化したものと同様の効果を得ることができる。

【0090】これに加えてビデオカメラ2は、素材毎に生成したデータ並替パターンに対応する素材特定暗号化鍵D13で暗号化しているので、仮に1つの暗号化データが解読された場合においても残り全ての暗号化データ1つ1つを再び解読させるようになされていることにより、結果として残り全ての暗号化データが直ちに解読されることを防止することができる。

【0091】一方、ネットワーク対応型暗号化システム1における暗号化鍵D10に対応する復号化鍵D20を予め内部に記憶しているビデオテープレコーダ3は、各素材であるエレメンタルストリームD1が入力される度にその各素材をそれぞれ特定するために生成されたUMIDデータD11と、当該UMIDデータD11に基づく各素材毎に固有な素材特定暗号化鍵D13でデータ並替パターンをそれぞれ暗号化することにより生成された暗号化データD16及びD17とを暗号化装置から取得し、各素材にそれぞれ対応するUMIDデータD11を暗号化鍵D10の数学的条件に合わせる変換を行うことにより素材特定復号化鍵D21を生成し、その素材特定復号化鍵D21で暗号化データD16及びD17をそれぞれ復号化することにより、暗号化装置で暗号化される前の元のデータ並替パターンを復元することができる。

【0092】以上の構成によれば、ネットワーク対応型暗号化システム1におけるビデオカメラ2では、各素材が入力される度にその各素材をそれぞれ特定するためのUMIDデータD11を暗号化鍵D10の数学的条件に合わせる変換を行うことにより得られた各素材毎に固有な素材特定暗号化鍵D13で、データ並替パターン(シャフリングテーブルデータD14及びインターリーブテーブルデータD15)をそれぞれ暗号化することにより、第三者にとっては暗号化鍵D10のアルゴリズム、また素材毎に特定されたUMIDデータD11

に基づいて素材特定暗号化鍵D13に変換する変換パターン、さらにはUMIDデータD11に含まれる固有な情報（マテリアルナンバ）の全てが分からなければ到底解読し得ない素材特定暗号化鍵D13を生成することができ、かくして、第三者によって容易にデータ並替パターンが解読されることを防止することができる。

【0093】なお、本実施の形態においては、インターネット4を経由して暗号UMIDデータD12、暗号化データD16及びD17をビデオカメラ2からビデオテーブルレコーダ3に送信する暗号化システムとしてのネットワーク対応型暗号化システム1に適用する場合について述べたが、本発明はこれに限らず、インターネット4に代えて、デジタル衛星放送等の有線及び無線通信媒体を経由しても良く、また図1との対応部分に同一符号を付して示す図12におけるパッケージメディア対応型暗号化システム50のように、メモ리카ード51を介して暗号UMIDデータD12、暗号化データD16及びD17をビデオカメラ2からビデオテーブルレコーダ3に受け渡すようにしても良い。

【0094】この場合ネットワーク対応型暗号化システム1においては、取得手段としてのCPU30（図10）が暗号UMIDデータD12、暗号化データD16及びD17をIEEE1394インターフェイス31から取得するが、パッケージメディア対応型暗号化システム50においては、取得手段としてのCPU30がIEEE1394インターフェイス31に代わる読み出し手段としてのメモ리카ードインターフェイスを介して取得するようにしても良い。

【0095】また上述の実施の形態においては、固有情報生成手段としてのCPU10及びUMID生成部21が固有情報としてのUMIDを生成し、当該UMIDのうちUMIDデータD11を抽出する場合について述べたが、本発明はこれに限らず、少なくともシリアルナンバ等の管理情報に乱数を乗じた固有情報を生成する固有情報生成手段であれば良い。このようにすれば、一段と少ないデータ量で素材である画像データを特定することができる。

【0096】さらに上述の実施の形態においては、CPU10及び素材特定暗号化鍵生成部23によって暗号化鍵生成手段を構成し、CPU30及び素材特定復号化鍵生成部42によって復号化鍵生成手段を構成する場合について述べたが、本発明はこれに限らず、他の種々の回路構成によって暗号化鍵生成手段及び復号化鍵生成手段を構成するようにしても良い。

【0097】さらに上述の実施の形態においては、暗号化手段としてのCPU10及びテーブル暗号化部25が暗号化対象としてのデータ並替パターンを暗号化することにより暗号化データD16及びD17を生成し、暗号復号化手段としてのCPU30及びテーブル復号化部43が当該暗号化データD16及びD17を復号化するこ

とにより元のデータ並替パターンを復元する場合について述べたが、本発明はこれに限らず、暗号化手段が記録ボタンが押下される度に入力した暗号化対象としての素材である画像データそのものを暗号化し、復号化手段素材が暗号化された当該素材である画像データを復号化するようにしても良い。

【0098】この場合インターネット4を経由してビデオテーブルレコーダ3に送信する情報としては、暗号UMIDデータD11のみで良い。

【0099】さらに上述の実施の形態においては、送信手段としてのCPU10及びIEEE1394インターフェイス11が固有情報としてのUMIDデータD11を暗号化することにより生成した暗号UMIDデータD12、暗号化データD16及びD17を送信し、受信手段としてのCPU30及びIEEE1394インターフェイス31が当該暗号UMIDデータD12、暗号化データD16及びD17を受信する場合について述べたが、本発明はこれに限らず、少なくとも固有情報と暗号化データとを送信する送信手段及び受信手段であれば良い。

【0100】さらに上述の実施の形態においては、非対象暗号化方式のRSAに従った暗号化鍵D10及び復号化鍵D20を用いる場合について述べたが、本発明はこれに限らず、例えば対象暗号化方式のDES(Data Encryption Standard)に従った暗号化鍵及び復号化鍵を用いる等、他の種々の暗号アルゴリズムに従った暗号化鍵及び復号化鍵を用いるようにしても良い。このようにすれば、インターネット対応型暗号化システム1を構築する状況に応じて、各種暗号アルゴリズムの特徴を効率よく選択することができる。

【0101】さらに上述の実施の形態においては、素材として画像データを適用する場合について述べたが、本発明はこれに限らず、例えば音声データ等、他の種々のデータを素材として適用することができる。

【0102】さらに上述の実施の形態においては、暗号化装置としてのビデオカメラ2及び復号化装置としてのビデオテーブルレコーダ3を適用する場合について述べたが、本発明はこれに限らず、例えば画像データや音声データ等の素材を編集するための編集装置、CD(Compact Disk)プレーヤやパーソナルコンピュータ等、他の種々の暗号化装置及び復号化装置に幅広く適用することができる。

【0103】

【発明の効果】上述のように本発明によれば、各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して各素材毎に固有な暗号化鍵を生成し、その暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化するようにしたことにより、類推し難い固有情報の全てが分からなければ第三者

にとっては到底解読し得ない固有な素材毎の暗号化鍵を生成することができ、かくして、第三者によって容易に暗号化対象が解読されることを防止することができる。

【0104】また各素材毎に対応した所定の情報として、各素材が入力される度にその各素材を所定データ量単位でそれぞれ並び替えるためのデータ並替パターンを暗号化するようにしたことにより、素材そのものを暗号化するよりも一段と少ないデータ量で暗号化することができる。

【0105】また上述のように本発明によれば、各素材が入力される度に当該各素材をそれぞれ特定するために生成された固有情報と、当該固有情報に基づく各素材毎に固有な暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化して生成された暗号化データとを暗号化装置から取得し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して暗号化データをそれぞれ復号化するための復号化鍵を生成し、その復号化鍵で暗号化データをそれぞれ復号化して各素材又は各素材に対応した所定の情報を復元することにより、類推し難い固有情報と、当該固有情報に基づいて生成されているために第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵とを取得して復号化鍵を生成することができ、かくして、確実に正確に各素材又は各素材に対応した所定の情報毎を復元することができる。

【0106】さらに上述のように本発明によれば、各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して各素材毎に固有な暗号化鍵を生成し、その暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化して暗号化データを生成し、暗号化データと固有情報とを送信する暗号化装置と、当該暗号化データと固有情報とを受信し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して暗号化データをそれぞれ復号化するための復号化鍵を生成し、その復号化鍵で暗号化データをそれぞれ復号化して各素材又は各素材に対応した所定の情報を復元する暗号復号化装置とを構築するようにしたことにより、暗号化装置では、類推し難い固有情報の全てが分からなければ第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵を生成することができるので、当該第三者によって容易に暗号化対象が解読されることを防止することができ、暗号復号化装置では、送信手段を介して類推し難い固有情報と、当該固有情報に基づいて生成されているために第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵とを受信して復号化鍵を生成することができるので、確実に正確に各素材又は各素材に対応した所定の情報毎を復元することができる。

【0107】さらに上述のように本発明によれば、各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成し、各素材にそれぞれ対応する固有情

報を所定の方式に従って変換して各素材毎に固有な暗号化鍵を生成し、その暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化して暗号化データを生成し、暗号化データと固有情報とを所定の記憶媒体に記憶する暗号化装置と、その暗号化データと固有情報とを当該記憶媒体から読み出し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して暗号化データをそれぞれ復号化するための復号化鍵を生成し、その復号化鍵で暗号化データをそれぞれ復号化して各素材又は各素材に対応した所定の情報を復元する暗号復号化装置とを構築するようにしたことにより、暗号化装置では、類推し難い固有情報の全てが分からなければ第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵を生成することができるので、当該第三者によって容易に暗号化対象が解読されることを防止することができ、暗号復号化装置では、記憶手段から読み出した類推し難い固有情報と、当該固有情報に基づいて生成されているために第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵とを受信して復号化鍵を生成することができるので、確実に正確に各素材又は各素材に対応した所定の情報毎を復元することができる。

【図面の簡単な説明】

【図1】本発明によるネットワーク対応型暗号化システムの構成を示す略線図である。

【図2】ディジタルビデオカメラレコーダの構成を示すブロック図である。

【図3】暗号化処理手順を示すフローチャートである。

【図4】UMIDのデータ構造を示す略線図である。

【図5】データ並替パターン決定画面を示す略線図である。

【図6】シャフリング処理の説明に供する略線図である。

【図7】シャフリング処理の説明に供する略線図である。

【図8】リードソロモン符号生成の際の説明に供する略線図である。

【図9】素材毎に記録された記録画像データと、暗号UMIDデータ及び暗号化データとの対応関係を示す略線図である。

【図10】ディジタルビデオテープレコーダの構成を示すブロック図である。

【図11】復号化処理手順を示すフローチャートである。

【図12】他の実施の形態におけるパッケージメディア対応型暗号化システムの構成を示す略線図である。

【符号の説明】

1、50……ネットワーク対応型暗号化システム、2……ビデオカメラ、3……ビデオテープレコーダ、4……インターネット、5……ビデオカセット、10、30……CPU、11、31……IEEE1394インターフ

22

\* ……テーブル暗号化部、27 ……記録部、33 ……HD  
D、36 ……デシャプリング部、37 ……デインターリ  
ープ部、40 ……鍵生成部、41 ……UMID復号化  
部、42 ……素材特定復号化鍵生成部、43 ……テー  
ブル復号化部、45 ……再生部。

【图 8】

## D2 VLCデータ

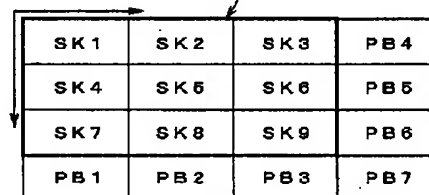


図8 リードソロモン符号の生成状態

## 2 デジタルビデオカメラレコーダ

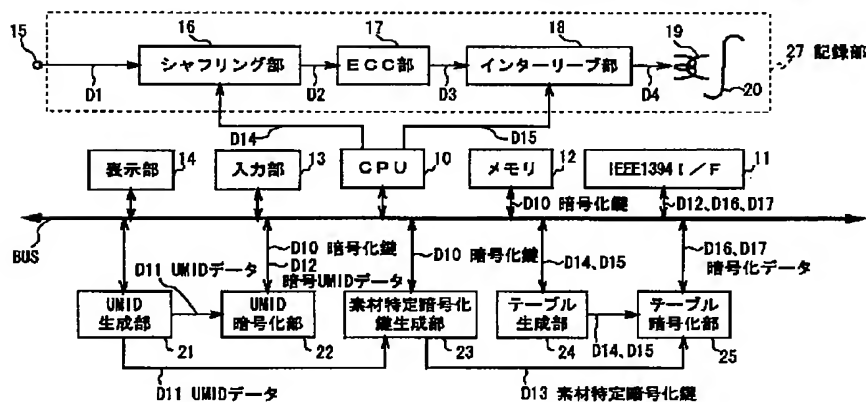


図2 デジタルビデオカメラレコーダの構成

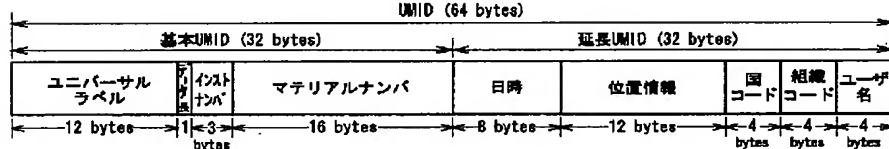
**UNID (64 bytes)**

図4 UMIDのデータ構造

【図3】

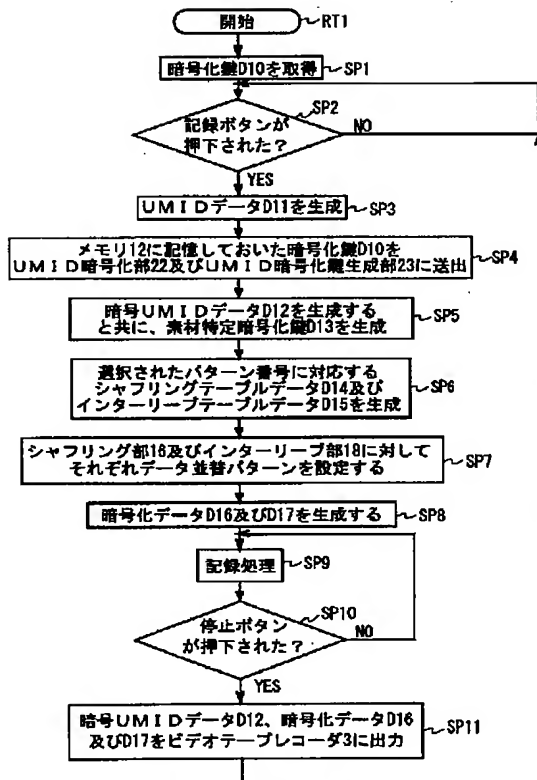


図3 暗号化処理手順

【図5】

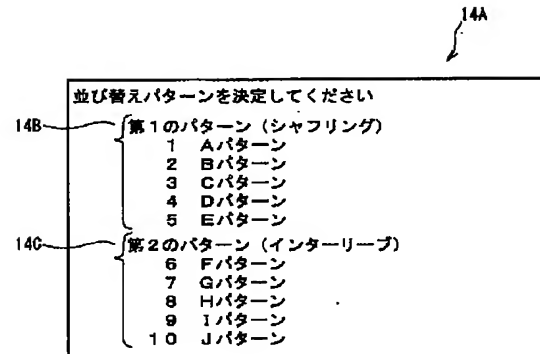


図5 データ並替パターン決定画面

【図7】

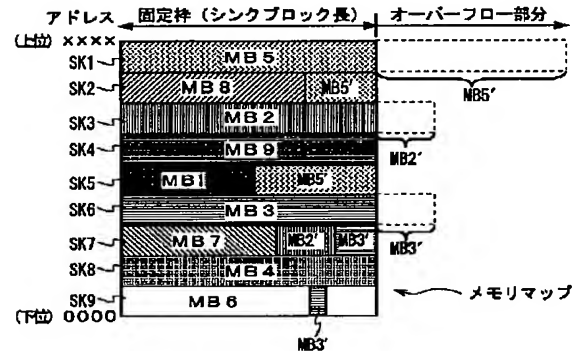


図7 シャフリング処理における内部メモリへの書き込み状況 (2)

【図6】

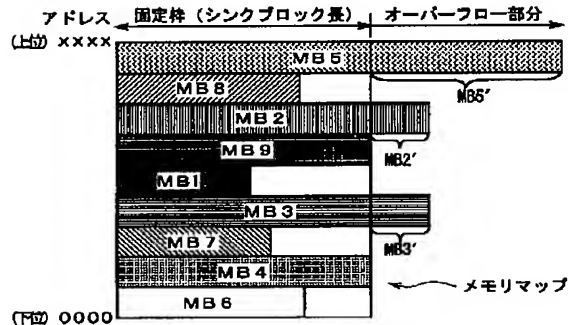


図6 シャフリング処理における内部メモリへの書き込み状況 (1)

【図9】

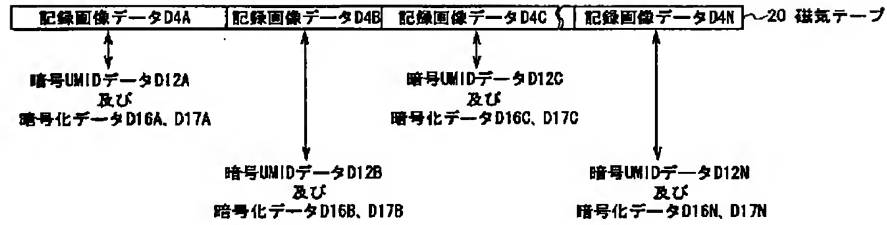


図9 素材毎に記録された記録画像データと、暗号UMIDデータ及び暗号化データとの対応関係

【図10】

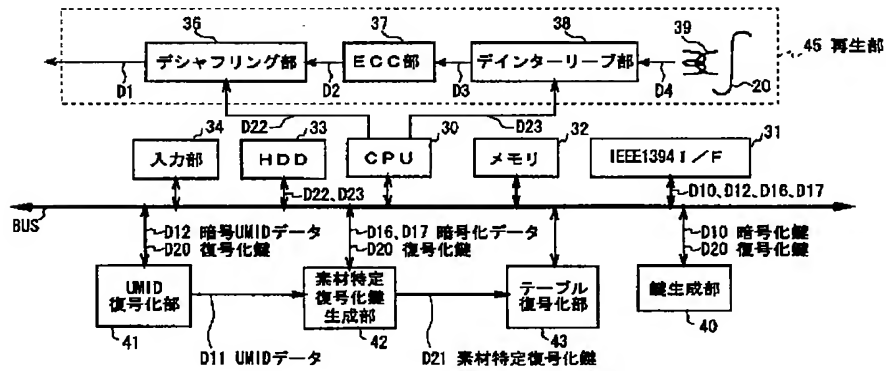


図10 デジタルビデオテープレコーダの構成

【図12】

50 パッケージメディア対応型暗号化システム

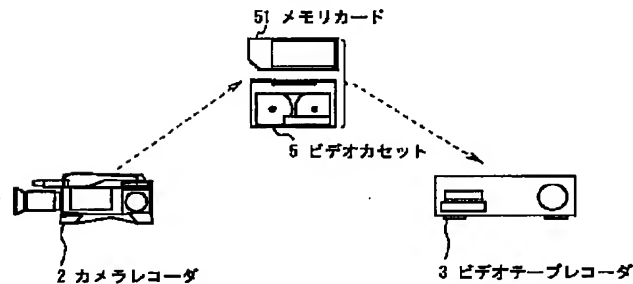


図12 他の実施の形態におけるパッケージメディア対応型暗号化システムの構成



【図11】

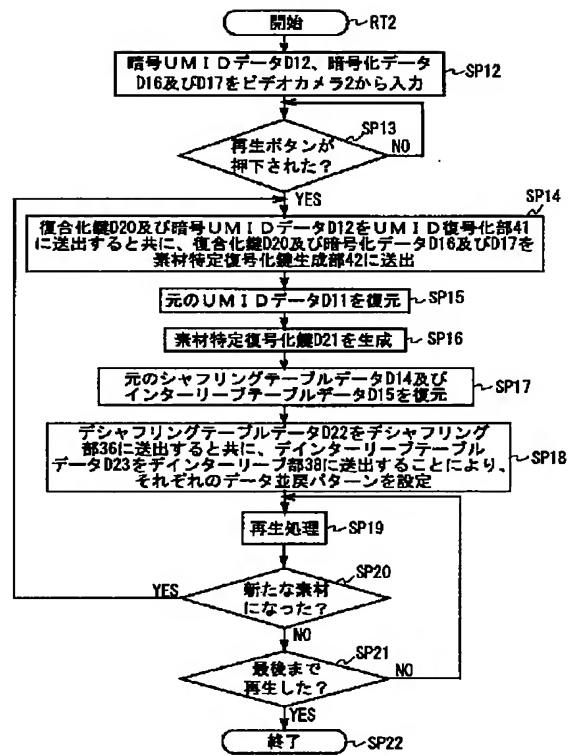


図11 復号化処理手順